Privacy impact assessment – a privacy protection improvement model?

Weber, Rolf H

25th IVR World Congress

LAW SCIENCE AND TECHNOLOGY

Frankfurt am Main

15–20 August 2011

Paper Series

No. 039 / 2012

Series B

Human Rights, Democracy; Internet / intellectual property, Globalization

Rolf H. Weber

Privacy Impact Assessment – A Privacy Protection Improvement Model?

URN: urn:nbn:de:hebis:30:3-248978

Conference Organizers:
Professor Dr. Dr. h.c. Ulfrid Neumann, Goethe University, Frankfurt/Main
Professor Dr. Klaus Günther, Goethe University, Frankfurt/Main; Speaker of the Cluster of Excellence "The Formation of Normative Orders"
Professor Dr. Lorenz Schulz M.A., Goethe University, Frankfurt/Main

Edited by:
Goethe University Frankfurt am Main
Department of Law
Grüneburgplatz 1
60629 Frankfurt am Main
Tel.: [+49] (0)69 - 798 34341
Fax: [+49] (0)69 - 798 34523

Rolf H. Weber, Zurich / Switzerland*

Privacy Impact Assessment – A Privacy Protection Improvement Model?

Abstract: A Privacy Impact Assessment (PIA) is a systematic risk assessment tool, enabling organizations to maintain compliance with data protection regulations, to manage privacy risks and to provide public benefits through the success of privacy-by-design efforts. An actual practical implementation of a PIA framework has been realized in the context of RFID applications encompassing detailed steps for the PIA process; a first successful review has been completed. The PIA also allows to introduce a pro-active mitigation of privacy risks through technical and organizational controls. The better the precautionary measures realize the relevant privacy objectives, the less likely will occur with the PIA process afterwards. The recent proposal for a far-reaching revision of the EU Data Protection Directive envisages to state a specific requirement to implement a PIA process. Indeed, since risks for privacy and non-disclosure of personal data are different in not identical circumstances, the protection measures should also be different, i.e. technology should assist in trying to achieve the (at least) second-best solution for the implementation of the data protection regime by a PIA. Insofar, privacy rules can be individualized and matched with the concrete needs in the given environment.

Keywords: Code-based regulation, Data Protection Directive, PIA process, PIA taxonomy, privacy-by-design, RFID applications, risk assessment, risk design, self-regulation

1. Introduction

Ten years ago, Jonathan Zittrain summarized the political economy of privacy: "With privacy, worry has come largely from individuals seeking protection against a whittling away of privacy by well-organized corporate interests."[1] In his seminal work "CODE version 2.0" Lawrence Lessig addresses the problem solving mechanisms of privacy by stating that the interests threatened would be diffuse and disorganized, notwithstanding the fact that the values of protection (security, combating cybercrime) would be compelling.[2]

* Professor of civil, European and commercial law at the Law Faculty of the University of Zurich, Switzerland, and Visiting Professor at the University of Hong Kong, Hong Kong, attorney-at-law (Zurich). The author is engaged as co-investigator in the research project "In Search of a Techno-legal Framework for the Protection of Personal Data", supported by the General Research Fund of the University of Hong Kong.

[1] Jonathan Zittrain, What the Publisher can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication, Stanford Law Review 52 (2000), 1206.

[2] Lawrence Lessig, CODE version 2.0, 2nd ed., 2006.

The term "privacy" has successfully defied at giving it a precise meaning.[3] On the one hand, privacy inevitably varies from society to society;[4] therefore, the existing rules show a patch-work of different provisions. On the other hand, privacy conveys a large number of concepts and ideas.[5] Generally looking, three basic features of privacy can be distinguished, namely (i) secrecy, i.e. information known about an individual, (ii) solitude, i.e. access to an individual, and (iii) anonymity, i.e. attention paid to an individual.[6] Concepts of privacy can be rooted in human dignity, breach of confidence relating to proprietary rights, and protection of individual autonomy from state interference.[7]

The law in the field of privacy is confronted with the problem that the Internet has overcome geographical boundaries; this fact causes the risk that the ethnographical uniqueness of society-driven privacy rules leads to a disparate picture of protection levels. Therefore, not surprisingly, a geographically-based regulatory approach can hardly cope with the requirements of an adequate online protection regime;[8] other models, not exclusively based on legal rules, need to be considered in building a framework of protection in consideration of the available technological means. Hereinafter, such a new approach, the Privacy Impact Assessment (PIA), executed by the concerned organization(s) will be discussed, i.e. an organizationally-based approach which eventually could overcome some weaknesses of the present legal framework. An appropriate assessment of the subject matter, however, needs to be embedded into the available set of regulatory models.

2. Regulatory Models for the Implementation of a Privacy Concept

Legislative actions in the privacy field can be taken at different levels. Apart from the (theoretical) possibility of no regulation at all, the choice is principally between the traditional national legislation, the international agreements incl. similar legal instruments and the self-

[3] Anne Cheung, Rethinking Public Privacy in the Internet: A Study of Virtual Persecution by the Internet Crowd, The Journal of Media Law 1(2) (2009), 191.

[4] The best indicator for this assessment is a comparison of the national rules on transborder data flows; thereto see the extensive list of Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Pri-vacy Law: Past, Present and Future, TILT Law & Technology Working Paper No. 016/2010, October 2010, Version: 1.0, Annex, online available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1689483.

[5] Samuel Warren/Louis Brandeis, The Right to Privacy, Harvard Law Review 4(5) (1890), 205 refer to the right „to be let alone"; see also Gus Hosein, Privacy as Freedom, in: Human Rights in the Global Information Society, ed. R.F. Jørgensen, 122-125 and 131-135.

[6] Raymond Wacks, Law, Morality, and the Private Domain, 2000, 238; Rolf H. Weber, Shaping Internet Governance: Regulatory Challenges, 2009, 239.

[7] Cheung (note 3), 193.

[8] Christopher Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law, OECD Digital Economy Papers, No. 187, 2011, OECD Publishing, 20, online available at: http://dx.doi.org/10.1787/5kg0s2fk315f-en.

regulatory approach. In addition, related to the online world, the model of a code-based approach has been developed.

The traditional national legislation is confronted with the major disadvantage of the limited scope due to the territoriality principle:[9] Domestic rules "only" apply within the boundaries of the concerned country (at least as long as an extraterritorial effect of the law is not envisaged) and have the consequence that a harmonized level of privacy protection cannot be achieved. Consequently, as it is the case today, national provisions in the privacy field request from da-ta-exporting persons and enterprises to comply with the principle of a comparable level of protection abroad.[10]

From a theoretical point of view, a transnational approach is inevitable in the online world.[11] Nevertheless, the development and implementation of internationally harmonized rules is hardly possible if societal perceptions vary so widely as in the case of privacy; since customary law can also not be built on the basis of diverging understandings of privacy, a successful harmonization of rules is not likely to happen. Therefore, internationally binding agreements related to privacy merely exist on a regional level (for example within the European Union). Other legal instruments only have non-binding character (being the case for the UN- and the OECD-Guidelines related to data protection). Fundamental freedoms in human rights conventions often encompass the right to privacy, but the principles are usually worded in a relatively vague way which makes their practical enforceability doubtful. Nevertheless, even if not all desirable principles work out as envisaged, experience with transnational law proves that global problems can be tackled by the international community,[12] which obviously means that the community should strengthen the efforts to negotiate and conclude additional treaties.[13]

Self-regulation follows the principle of subsidiarity, meaning that government intervention should only take place if participants of a specific community are not able to find suitable solutions (structures, behaviors) themselves; since, however, public law defines the contours of private law, it contains aspects of the role of self-regulatory mechanisms.[14] The legitimacy of self-regulation lies in the fact that private incentives lead to a need-driven rule-setting process. A major advantage of self-regulation can be seen in the possibility to develop and establish rules independent of the principle of territoriality; other strengths are the

[9] For a general overview see Rolf H. Weber, Regulatory Models for the Online World, 2002, 57 et seq.
[10] Kuner (note 8), 21.
[11] Weber (note 9), 77.
[12] Stuart Biegel, Beyond our control? Confronting the Limits of our Legal System in the Age of Cyberspace, 2001, 184.
[13] Weber (note 9), 77.
[14] Weber (note 9), 79.

efficiency in responding to real needs and mirroring the technology, the openness for a permanent consultation process and for a timely adaption of rules in case of changing technologies, as well as the existence of incentives for compliance with a "self-given" legal framework.[15] Disadvantages of self-regulation, however, should not be overlooked: The quality of the "legislative" process can hardly be judged under the angle of a democratic participation (problem of outsider), "private norms" are not generally binding in legal terms, self-regulatory mechanisms are not always stable, and – in particular – this kind of legal framework does hardly know enforcement procedures leading to sanctions in case of non-compliance.[16]

In the light of a perceived dissatisfaction with the available regulatory models, Lawrence Les-sig developed a new, more technically-oriented approach, the so-called "code-based regulation", for the online world some 10 years ago.[17] According to Lessig, human behavior is regulated by a complex interrelation between four forces, namely law, markets, social norms and architecture.[18] Code solutions, similar to legal rules, principally reflect "information" that allocates and enforces entitlements. The design of the code materially influences human behavior since architecture is one of the four regulators; depending on the architecture certain activities will be possible or difficult to carry out.[19] Therefore, Lessig arrives at a world in which code can do much of "the work that the law used to do far more effectively than the law did."[20] Consequently, effective regulatory power shifts from law to code based on an effective architectural framework.[21] Lessig's approach that relates the code/architecture to the control paradigm has not remained uncontested: For example, the aspect of established control structures has a political impact; furthermore, courts impose checks on the powers of private regulators where such regulation threatens important collective values.[22]

The below discussed Privacy Impact Assessment draws on two or even three of the described regulatory models: Technical designs are the basis for implementing privacy standards, self-regulatory provisions give the legal framework for the establishment of the rule-setting mechanisms and some general surveillance functions for compliance purposes are laid down in an at least regionally binding legal instrument. This combination of technical and

[15] Weber (note 9), 80, 83-84.
[16] Weber (note 9), 84-85.
[17] Lawrence Lessig, Codes and other Laws of Cyberspace, 1999, 3 et seq.
[18] Lessig (note 17), 88.
[19] Lessig (note 17), 129.
[20] Lessig (note 17), 130.
[21] Lessig (note 17), 296.
[22] See Victor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, 2009, 145/46; see also Weber (note 9), 99.

legal sources helps realizing the successful implementation of an adequate privacy environment's framework.

3. Elements of a Privacy Impact Assessment

3.1 Notion and Benefits

A Privacy Impact Assessment (PIA) is generally regarded as a systematic risk assessment tool that can be usefully integrated into a decision-making process, evaluating a proposal in term of impact on personal data privacy with the objective of avoiding or minimizing adverse effects.[23] A PIA offers the data users an "early warning" system since privacy problems might be identified and detected prior to the implementation of certain systems.

The benefits in conducting a PIA encompass the possibility (i) to establish and maintain compliance with privacy and data protection laws and regulations, (ii) to manage privacy risks within an organization and in relation to third persons, and (iii) to provide public benefits through the success of privacy-by-design efforts.[24] In addition, a PIA is useful in enabling to adequately consider the impact of an action on personal data privacy, directly addressing the privacy problems in the process, providing solutions or safeguards at the design stage and benchmarking for future privacy compliance audit and control, being a cost-effective way of reducing privacy risks as well as providing a credible source of information to allay any privacy concerns from the public and the stakeholders.[25]

Apart from the below thoroughly discussed (and most detailed) PIA related to RFID applications within the European Union, other authorities have also issued general leaflets and guidelines[26] or have dealt with the PIA in connection with specific issues such as public security[27] or e-government.[28]

3.2 Example of RFID

An extensive and still ongoing PIA project concerns the Radio Frequency Identification (RFID) applications. On May 12, 2009, the European Commission issued a Recommendation

---

[23] See Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong, Privacy Impact Assessment (PIA), July 2010, 1, online available at: http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf; see also Australian Government, Office of the Privacy Commissioner (OPC), Privacy Impact Assessment Guide, August 2006, 4, online available at: www.privacy.gov.au/publications/PIA06.pdf.

[24] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, 3, online available at: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf.

[25] PCPD Hong Kong (note 23), 1.

[26] For example PCPD Hong Kong (note 23) and Australian OPC (note 23).

[27] See US Department of Homeland Security, State, Local, and Regional Fusion Center Initiative, Privacy Impact Assessment, December 11, 2008, online available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ia_slrfci.pdf.

[28] See for example the United States E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002).

on the implementation of privacy and data protection principles in applications supported by RFID.[29] This Recommendation should become the basis for developing a framework related to privacy impact assessments by the industry, in collaboration with all relevant stakeholders, and supervised by the Article 29 Data Protection Working Party.[30] On March 31, 2010, industry representatives delivered a PIA framework proposal which has been reviewed and partly rejected for improvement by the Article 29 Data Protection Working Party. The second proposal has then been approved on February 11, 2011.[31] In April 2011, the "inauguration" of the PIA framework on RFID applications was formally enacted and in November 2011 a first review of the actual implementation has taken place.

In the understanding of the EU authorities the PIA should be designed on the basis of the following taxonomy:[32]

- The PIA is to be introduced as a process making the assessment of privacy impacts of certain activities a conscious and systematic effort.
- The framework should identify the objectives of the (RFID) applications as well as the common structure and content of such applications.
- A PIA report must be made available documenting the PIA process and addressing the review steps of its implementation.
- PIA templates may be developed based on the framework to provide industry-based, application-based, or other specific formats for PIA processes.

According to the relevant documentation, the PIA process related to RFID applications is constructed in two phases:[33]

- A pre-assessment phase classifying the RFID applications according to a four level scale, based on a decision tree.
- A risk assessment phase, broken down in four main steps, namely (i) characterization of the application (data types, data flows, RFID technology, data storage and transfers, etc.), (ii) identification of the risks to personal data and evaluation of the threats (likelihood and

[29] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf.
[30] See also Rolf H. Weber/Romana Weber, Internet of Things: Legal Perspectives, 2010, 45/46.
[31] Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, 00327/11/EN, WP 180.
[32] PIA Framework (note 24), 4.
[33] Opinion 9/2011 (note 31), 4/5.

potential impact), (iii) identification and recommendation of controls, in response to previously identified risks, and (iv) documentation of the results of the PIA process (incl. conditions for review and information concerning residual risks).

Furthermore, the relevant documentation requests the PIA application operators to establish their own internal procedures in view of supporting the execution of the PIA processes, encompassing for example the following steps:[34]

- Scheduling of the PIA process in order to plan the necessary executions and adjustments in time and in compliance with industry requests and the supervision by the competent authorities;
- Internal review of the PIA process (incl. the initial analysis) and of the PIA reports in view of the compliance with the applicable documentation and the factual implementation of the relevant measures;
- Compilation of supporting artifacts (for example results of security reviews, control designs) as evidence that the processes are executed in a proper way;
- Determination of the persons and/or functions within the organization who have the authority for relevant actions during the PIA process;
- Provision of criteria of how to evaluate and document whether the actual applications are ready for deployment consistent with the PIA framework and any relevant PIA template;
- Consideration/identification of factors that would require a new or revised PIA process, for example due to significant changes in the applications, failures in the processes, weaknesses in implementation measures, etc.
- Stakeholder consultation in order to receive the appropriate feedback from all directly or indirectly involved persons/organizations/authorities and, thereupon to be in a position of improving the PIA process.

If issues or even problems occur, a specific corrective action plan needs to be developed; relevant risks identified should be appropriately mitigated in order to assure that no significant residual risks remain and a new PIA might have to be executed.[35]

[34] PIA Framework (note 24), 4/5.
[35] PIA Framework (note 24), 10.

3.3 Risk Design Issues

The objective of a risk assessment is to identify the privacy risks caused by specific processes or applications; the discussed RFID applications are a new technological tool, but may only serve as an example since privacy risks occur in virtually every business and in government. Therefore, the development of an adequate and appropriate risk design is crucial.

In the context of a PIA, privacy risks are to be concretely identified. Notwithstanding the fact that each industry or business is confronted with some specific privacy risks it seems to be possible to list "critical factors" which might be applicable in virtually all market segments. On that note, the following privacy risks should be taken into consideration:[36]

- No data collections for unspecified and unlimited data collections;
- No data collections exceeding their purpose;
- Avoidance of incomplete information and lack of transparency;
- No combinations of data collections exceeding the given purpose of collection;
- Lack of erasure policies or mechanisms;
- Avoidance of invalid explicit consent to data collection (for example threat);
- No secrete data collection;
- Avoidance of a situation of inability to grant access;
- No technical/operational measures preventing objections by data subjects;
- Lack of transparency of automated individual decisions;
- Insufficient access right management;
- Insufficient authentication mechanisms;
- Illegitimate data processing;
- Insufficient logging mechanisms;
- Uncontrollable data gathering.

Seen from the angle of the data subject, the relevant factors of privacy risks which are to be taken into account encompass (i) the functions and activities of the data users, (ii) the nature of the personal data involved, (iii) the number of individuals affected, (iv) the gravity of harm caused in case of improper handling of data protection rules and (v) the compliance with the privacy standards contained in applicable codes, policies, practices and regulations.[37]

[36] The list of privacy risks follows the PIA Framework (note 24), Annex III.
[37] PCPD Hong Kong (note 23), 2.

Ideally, already at an early stage of a system's development the efforts should be directed to a pro-active mitigation of risks through technical and organizational controls.[38] The better the precautionary measures realize the requested privacy objectives, the less likely problems will occur during the PIA process afterwards. Sometimes, PIA leaflets of data protection authorities contain valuable lists of possible measures for avoiding and mitigating privacy risks.[39]

Risk assessment processes are known from many segments of the industry, mainly the high-technology and also the health fields. Lessons learned could be that risk assessments should be run at an early stage prior to the decision of definitely implementing certain systems, that measures susceptible to malicious attacks should be avoided and applications already configured in a privacy friendly way should get a special preference.

Generally looking, despite the difficulties, it is unavoidable that in addition to the identification of the risks, a PIA process includes a relative quantification of the risks, i.e. the PIA operator must consider, as informed by the principle of proportionality and under reasonable conditions, whether privacy risks are likely or not likely to realize in the processes executed in the business.[40] Such kind of risk assessment requires evaluating the applicable risks from a privacy perspective, encompassing the significance of the risk, the likelihood of its occurrence and the magnitude of the impact (low, medium, high) in case of its occurrence.

A general important problem in the risk assessment context concerns the uncertainties and complexities inherent in risk analyses and the use of science (technology) policies. Usually, three aspects of scientific evaluation are taken into account:[41] (i) balancing categories of evidential reasoning, (ii) judging data and theories, and (iii) considering desiderata of rationality. The balancing categories concern how to weigh different risk estimates; judging data encompasses the determination of quality of data and theories used, depending on statistical proper-ties, methodology, reliability, relevance and the level of scrutiny by the scientific community. Rationality is described as including conceptual clarity for all terms used in the discourse, logical deduction, methodological rigor, practicality, ontological realism, epistemological reflection, and valuation.

So far, experience with the application of PIA is still limited and knowledge must be gained in practice. The first review of the efforts related to the RFID PIA in November 2011,

[38] PIA Framework (note 24), 7.
[39] See for example PCPD Hong Kong (note 23), 2.
[40] PIA Framework (note 24), 9.
[41] See for example Douglas Crawford-Brown/Joost Pauwelyn/Kelly Smith, Environmental Risk, Precaution, and Scientific Rationality in the Context of WTO/NAFTA Trade Rules, Risk Analysis 24 (2004), 461, 465.

however, gives at least some confidence that this instrument could also be used in other contexts.[42]

4. Revision of the EU Directive: Implementation of PIA

In the course of the fundamental revision of the EU Directive on Data Protection 95/46[43] which has been launched on January 25, 2012,[44] the EU Commission proposes to include a specific provision related to a data protection impact assessment into the future legal framework in the newly drafted Data Protection Regulation.[45] Art. 33 para. 1 of the proposal reads as follows:

> "Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."

Thereafter, the proposed provision lists specific (data protection) risks in case of data processing (para. 2), followed by the conditions to be fulfilled by the impact assessment (para. 3), namely the description of the envisaged processing operations and of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data. Furthermore, addition-al provisions regulate the exchange of views on a PIA and the supervision by the competent authorities (paras 4-7).

The outcome of the legislative process is obviously not yet known. However, the opposition to a pre-final draft of the legal framework which unintendedly surfaced in November 2011 to the public mainly concerned with regard to the form (Regulation instead of Directive), the introduction of new fundamental rights (such as the right to be forgotten) and

[42] Sarah Spiekermann, The RFID PIA – developed by industry, agreed by regulators, in: Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy, ed. D. Wright/P. de Hert, 2012, 9, pre-publishing version, online available at: http://ec.europa.eu/information_society/policy/rfid/documents/pia_spiekermann.pdf.

[43] European Parliament, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on Free Movement of such Data, 1995, online available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF.

[44] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft, 2012, online available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[45] A Regulation of the EU would be directly applicable in the Member States, in contrast to a Directive which has to be implemented in national law; nevertheless, the competence of the EU to release a Regulation in the data protection field is hotly debated and highly contested.

the extended supervisory regime with massive powers of data protection surveillance authorities, but it was not directed against the principle of a privacy impact assessment. Therefore, the fair assumption might be expressed that the PIA is going to survive the legislative process and will come into force, expectedly in 2014.

5. Merits of PIA on the Way to Privacy-by-Design

In principle, the privacy impact assessment has the regulatory benefit of encompassing two (perhaps even three) regulatory models: Mainly the PIA relies on the self-regulatory approach, but based on a "code-related" notion since technology plays a major role. In addition, compliance with the applicable legal framework is supervised by the authorities. Thereby, the strengths of each model can be combined and the weaknesses minimized.

Since an international harmonization of data protection laws might be unlikely to happen during this decade, the merits of a well-drafted privacy policy by the concerned entity (business, government) should not be underestimated, particularly since guidelines and models are available and experiences have already be gained.[46] This assessment goes along with the fact that according to studies related to regulations governing the transborder flows of data an organizationally-based approach making data exporters accountable for ensuring the continued protection of personal data is the most viable tool for an appropriate privacy framework.[47] Obviously, adequate governing practices within the organization must be put in place and, even more, accountability measures are to be implemented.[48]

In order to improve the privacy legal framework it has been proposed by legal scholars to turn to a "IT-security legislation" approach.[49] This concept encompasses initiatives that demand the establishment of reliable IT-security standards which should protect from unauthorized dis-closure of data; for example, new industry-based technological standards could introduce stringent safeguards. Thereby, technological "norms" would delineate a legal concept in which a broad scale of privacy problems can be designated.[50] Such kind of approach has the advantage of leading to a concept of relational privacy taking into account

[46] For further details see Rolf H. Weber, How Does Privacy Change in the Age of the Internet, In: Internet and Surveillance: The Challenges of Web 2.0 and Social Media, ed. C. Fuchs/ K. Boersma/A. Albrechtslund/M. Sandoval, 2012, 280.
[47] Kuner (note 8), 20 and 26.
[48] PIA Framework (note 24), 17 and 19.
[49] See Weber (note 46), 283 and 286.
[50] See Daniel J. Solove, A taxonomy of privacy, University of Pennsylvania Law Review 154(3)(2006), 477 et seq.; Weber (note 46), 286.

the specific demands of the manifold data subjects.[51] Furthermore, the implementation of an adequate PIA could eventually mitigate civil liability.[52]

From a technological angle a pro-active integration of privacy principles in a system's design should be achieved in the form of privacy-by-design.[53] This term can be defined as a pro-active engineering and management approach enabling a selective and sustainable minimization of information systems' privacy risks through technical and governance controls.[54]

The seven fundamental principles of privacy-by-design are:[55]

- Proactive not Reactive; Preventive not Remedial;
- Privacy as the Default Setting;
- Privacy Embedded into Design;
- Full Functionality – Positive-Sum, not Zero-Sum;
- End-to-End Security – Full Lifecycle Protection;
- Visibility and Transparency – Keep it Open;
- Respect for User Privacy – Keep it User-Centric.

A privacy-by-design framework should be composed of privacy-friendly architectures and technically enforceable default policies (i.e. opt-in settings) or data scarcity policies (i.e. erasure or granularity policies), data portability and user access- and delete-rights.[56] The so far developed PIA concepts which now are even proposed as legislative action in the context of the revised EU Data Protection Regulation enables businesses to have privacy embedded in the system development life cycle and hence in organizational processes by embracing the respective domain.[57]

[51] See Pieter Kleve/Richard De Mulder, Privacy protection and the right to information: a search of a new symbiosis in the information age, in: Cyberlaw & security privacy, ed. S. Kierkegaard, 2nd ed., 2007, 340.
[52] See Raphaël Gellert/Dariusz Kloza, Can Privacy Impact Assessment Mitigate Civil Liability? A "Precautionous" Approach, IRIS 2012, conference proceedings.
[53] This term has been coined by Ann Cavoukian, Information & Privacy Commissioner Ontario, Canada, Privacy by Design: The 7 Foundational Principles, online available at: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.
[54] See Sarah Spiekermann, The Challenges of Privacy-by-Design, Communications of the ACM, Viewpoint, forthcoming in 2012, 1.
[55] Cavoukian (note 52), 2.
[56] Spiekermann (note 53), 3-4.
[57] Spiekermann (note 53), 4.

Summarizing, the Privacy Impact Assessment enables the concerned entities to design the conditions of the framework according to the individual needs. Since the risks for privacy and non-disclosure of personal data are different in not identical circumstances, the protection measures should also be different, i.e. technology as precautionary means should assist in trying to achieve the (at least) second-best solution for the implementation of the data protection regime by a PIA. Insofar, privacy rules can be individualized and matched with the concrete needs in the given environment.

Address: Prof. Dr. Rolf H. Weber, University of Zurich, Rämistrasse 74/38, 8001 Zurich / Switzerland.